Computer Forensics LLC
1880 North Congress Ave, Suite 333
Boynton Beach, Florida 33426
Main: 561.404.3074
www.ComputerForensicsLLC.com

Reference Malibu Case Raleigh

I received FedEx package tracking number 772371638455 on 12/26/2014 from Tim Kiefer D4 Data in Rochester, NY. The package contained one Western Digital HDD (hard disk drive). The Western Digital HDD was encrypted with TrueCrypt software. I was provided the password to unencrypt the HDD. Once the HDD was unencrypted I noticed it had several folders on the drive including EnCase images of 2 hard drives listed as belong to Mr. Raleigh. The drive also contained 2 Cellebrite iPad extractions along with photographs of the devices.

Name	Date modified	Type	Size
iPad Backup	12/5/2014 12:13 PM	File folder	
iPad2	12/10/2014 10:49 ...	File folder	
JRaleigh_LT1	12/5/2014 5:31 AM	File folder	
JRaleigh_RT2	12/4/2014 9:18 PM	File folder	
901014580 JRaleigh Photos	12/10/2014 2:25 PM	Compressed (zipp...	7,486 KB

EnCase D4 Data Imaging Summary "JRaleigh_LT1" aka "MacBook C02HW056DV31"

Name	MacBook C02HW056DV31
Actual Date	12/03/14 08:07:41PM
Target Date	12/03/14 08:07:41PM
Case Number	90-1014-580
Evidence Number	Not provided
Examiner Name	Molly Heaven-Hoyle
Notes	Not provided
Model	APPLE HDD HTS541010A9E682
Serial Number	J8200076GN56NA
Drive Type	Fixed
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	23201464e479650b4a4018536c792072
Verification MD5	23201464e479650b4a4018536c792072
Acquisition SHA1	eb3a32e6fb0e95c4930e18404c2ae4b4b99972e4
Verification SHA1	eb3a32e6fb0e95c4930e18404c2ae4b4b99972e4
GUID	b9360c5362d042cb8c44a73482485d3d
Read Errors	0
Missing Sectors	0
Disk Elements	No
CRC Errors	0
Compression	Good
Total Size	1,000,204,886,016 Bytes (931.5GB)
Total Sectors	1,953,525,168
Disk Signature	00000000
Partitions	Valid

EnCase D4 Data Imaging Summary "JRaleigh_RT2" aka "MacBook 340269NBATM"

Name	MacBook 340269NBATM
Actual Date	12/03/14 04:02:13PM
Target Date	12/03/14 04:02:13PM
Case Number	90-1014-580
Evidence Number	Not provided
Examiner Name	Molly Heaven-Hoyle
Notes	Not provided
Model	Hitachi HTS545050B9A300
Serial Number	101112PBN475X7C13R1L
Drive Type	Fixed
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	84b893f00da4a899568768cbb1a77729
Acquisition SHA1	05d8a75544f18968d79ffcf9e3d67e21f1db3691
Verification SHA1	05d8a75544f18968d79ffcf9e3d67e21f1db3691
GUID	cc6f062f4e9741c09d1d662845827a48
Read Errors	0
Missing Sectors	0
Disk Elements	No
CRC Errors	0
Compression	Good
Total Size	500,107,862,016 Bytes (465.8GB)
Total Sectors	976,773,168
Disk Signature	00000000
Partitions	Valid

JRaleigh_LT1" aka "MacBook C02HW056DV31

Time Zone Settings

JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\private\etc\localtime
Configured Time Zone:America/Detroit

```
/usr/share/zoneinfo/America/Detroit
```

OS Information

```
ProductBuildVersion: 14B25
ProductCopyright: 1983-2014 Apple Inc.
ProductName: Mac OS X
ProductUserVisibleVersion: 10.10.1
ProductVersion: 10.10.1
```

User Information

	Name	File Ext	Last Accessed	File Created	Full Path
1	.localized	localized	09/09/14 06:16:34PM	09/09/14 06:16:34PM	JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\.localized
2	Guest		10/17/14 11:40:29AM	10/17/14 11:40:27AM	JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\Guest
3	jr		12/02/14 11:19:00PM	07/27/10 12:51:33AM	JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr
4	macports		07/01/12 10:28:38AM	03/01/12 10:11:52AM	JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\macports
5	Shared		10/17/14 10:37:15AM	06/24/11 05:49:24PM	JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\Shared

JRaleigh_LT1" aka "MacBook C02HW056DV31 Findings:

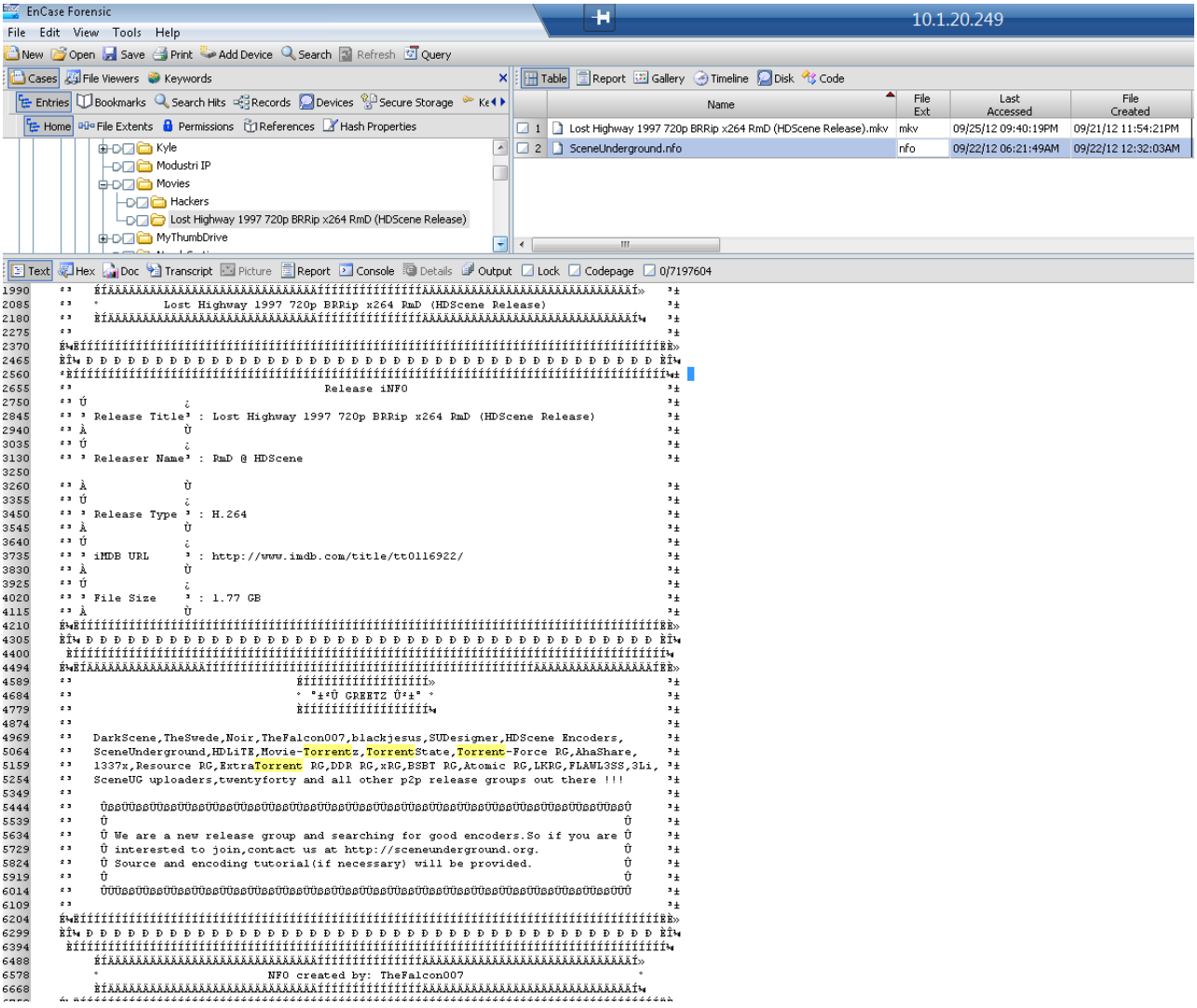
A search of the hard drive for evidence relating to Malibu Media movies was negative. A search of the hard drive evidence of BitTorrent use was positive as outlined in this report.

1. Using IEF (Internet Evidence Finder Software by Magnet Forensics) I located hundreds of "Cloud Services" related URLs (Web Addresses) relating to sites like Dropbox and Google Drive. Please review the final case files folder "Cloud Services URLs" for complete list.

2. Using IEF I located several Adium, skype and chats about BitTorrent (Adium is a free instant messaging application for Mac OS X). Please review the final case files folder "Complete List Adium Chats" for complete list and for a list of just the chats pertaining to the keyword Torrent please review the folder "IEF Torrent Keyword Search Hits".

3. Using IEF I located several Skype & iMessage chats messages about Torrents, hacking etc. Please review the final case files folder "IEF Torrent Keyword Search Hits" for complete list.

4: EnCase Screen Capture showing the related "NFO" file. NFO files are commonly associated with copyright infringement files and are often included with the infringed file(s).



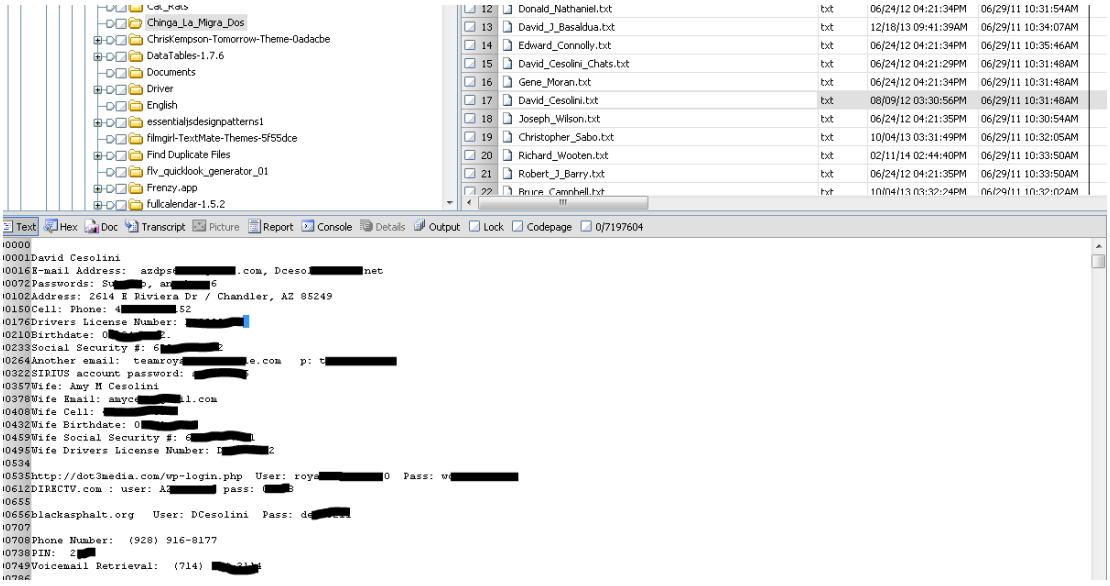
1) File Name: Lost Highway 1997 720p BRRip x264 RmD (HDScene Release).mkv
Last Accessed: 09/25/12 09:40:19PM
File Created: 09/21/12 11:54:21PM
File Full Path: JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Desktop\Movies\Lost Highway 1997 720p BRRip x264 RmD (HDScene Release)\Lost Highway 1997 720p BRRip x264 RmD (HDScene Release).mkv

2) File Name: no country for old men [vose] dvdrip xvid mp3.avi
Last Accessed: 11/04/13 09:43:05AM
File Created: 01/03/12 09:53:01PM
Full Path: JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Desktop\Movies\no country for old men [vose] dvdrip xvid mp3.avi

Using EnCase software a keyword search for "torrent" was conducted. Upon examining the search hits I located a text file named "David_Cesolini_Chats.txt" that contained a discussion about torrents. Further examination revealed that this chat and other files contained in a folder "Chinga_La_Migra_Dos" may be related to a hacking event that took place in 2011. This computer contains the sensitive files released by hacker(s) which contain individuals' personal information including social security, driver's license numbers, account passwords etc.

```
177880 David: yeah - whassup?
1779049:35 PM me: just checked my torrent
177940  1.5MB
177948  download speed
177965  hahahahahaha
177980 David: i think i have a crappy torrent
178020  i'm at 1.2kb
178035 me: lol
178044  i also have 120 seeders
178070 David: you and your seeders
1780999:36 PM me: dork
178116  this is now a new movie
178142  The Book of Eli
178160 David: i should try to get toy story 3
178200 me: its not out yet
178221  I only want things with excellent quality and excellent sound. cause i watch them through my PS3
1783209:37 PM David: i'm downloading toy story 3 now - it's going much faster. i'll let you know if it's good
1784249:38 PM you go through isohunt?
178456 me: do you keep all your downloads after use or delete
178512 David: delete
178527 me: i do a google search for a torrent
178567  either piratbay or kickasstorrent
178603 David: cool
178616 me: isohunt sometimes
178639 David: gotta be careful for viruses
178676 me: agree
1786879:39 PM kickass usually has the better stuff
178732  i delete everything in the torrent besides the movie. then transfer to ps3, I dont open it on my pc at all.
178842  so most virus if any are formated for pc's
1788879:40 PM David: gotcha - although if you get a ps3 virus, you're screwed. how do you clean a ps3??
178985 me: just format. so I loose my saved data boohoo
1790359:41 PM and if it brakes its under warranty
1790799:42 PM David: when am i getting froyo?
179119 me: i want to find a new version of Chrome OS. But nothing you would think something wouldve gotten leaked by now.
179236  Thats a good question
179260  hahaha
JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Scrap Pile\Old Swap Drive\Chinga_La_Migra_Dos\David_Cesolini_Chats.txt (PS 820063431 LS 819653791 CL 102456723 SO 236 FO 179948 LE 1)
```

EnCase screen capture of sensitive data relating to "Chinga_La_Migra_Dos" redacted:



Located Torrent Files

1) File Name: test.torrent
Last Accessed: 09/04/14 02:43:50PM
File Created: 03/18/14 02:49:46PM
Full Path: JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Applications\Development\LightTable\LightTable.app\Contents\Resources\app.nw\core\node_modules\bencode\benchmark\test.torrent

2) File Name: xubuntu-13.04-desktop-i386.iso.torrent
Last Accessed: 09/15/14 08:57:29AM
File Created: 04/25/13 06:28:19AM
Full Path: JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Downloads\xubuntu-13.04-desktop-i386.iso.torrent

Windows XP Parallels Virtual Machine Located in the following location:

1. JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Documents\Parallels\Windows 7.pvm\Windows 7-0.hdd\Windows 7-0.hdd.0.{5fbaabe3-6958-40ff-92a7-860e329aab41}.hds
2. JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\Users\jr\Documents\Parallels\Windows XP Old.pvm\Windows XP.hdd\Windows XP.hdd.0.{5fbaabe3-6958-40ff-92a7-860e329aab41}.hds

Parallels Desktop software is hardware virtualization software for the MAC operating system. Parallels software allows the user to create and run virtual operating systems including Windows based operating systems on a MAC computer. In this case the user was utilizing a Microsoft Windows XP virtual machine with Parallels Software. Using EnCase software I copied out the virtual machine "Windows XP.hdd.0.{5fbaabe3-6958-40ff-92a7-860e329aab41}.hds" along with the companion configuration files to my local forensics machine. Using software "VMware vCenter Converter Standalone Client" I converted the image to a VMware virtual machine and loaded the image into IEF forensic software for processing. The same process was followed for the Windows 7 Parallels virtual machine however the configurations appeared to be corrupt.

Operating System Information

Operating System	Microsoft Windows XP
Operating System Version	-Not Found-
Build Number	2600
Version Number	5.1
Product ID	76487-OEM-0054883-52515
Product Key	DQGQ7-R6MVP-KPBKY-PWY88-47FYJ
Last Service Pack	Service Pack 3
Owner	Jesse Raleigh
Organization	(not found)
Install Date/Time - (UTC-7:00) (MM/dd/yyyy)	07/22/2010 10:44:09 AM
Last Shutdown Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/23/2014 10:38:58 AM
System Root	C:\WINDOWS
Path	C:\WINDOWS
Source	Raleigh.vmdk - Partition 1 (Microsoft NTFS, 7 GB) (All Files and Folders) - [ROOT]\WINDOWS\system32\config\software
Located At	Registry Key: Microsoft\Windows NT\CurrentVersion, ControlSet001\Control\Windows
Evidence Number	Raleigh

User Account Information

User Name	Type of User	Security Identifier	User Group(s)	Last Login Date/Time - (UTC-7:00) (MM/dd/yyyy)	Last Password Change Date/Time - (UTC-7:00) (MM/dd/yyyy)	Login Count	Account Disabled	Password Required
Administrator	Local User	500	Administrators		07/22/2010 06:31:25 AM	0	False	True
Guest	Local User	501	Guests			0	True	False
HelpAssistant	Local User	1000			07/22/2010 10:35:04 AM	0	True	True
SUPPORT_3889	Local User	1002	HelpServicesGroup		07/22/2010 10:38:42 AM	0	True	True
Jesse	Local User	S-1-5-21-789336058-	Administrators	01/23/2014 10:38:12 AM	07/22/2010 10:56:37 AM	371	False	True
ASPNET	Local User	1004	Users		10/21/2013 08:25:55 AM	0	False	False

Windows XP Parallels Virtual Machine Findings

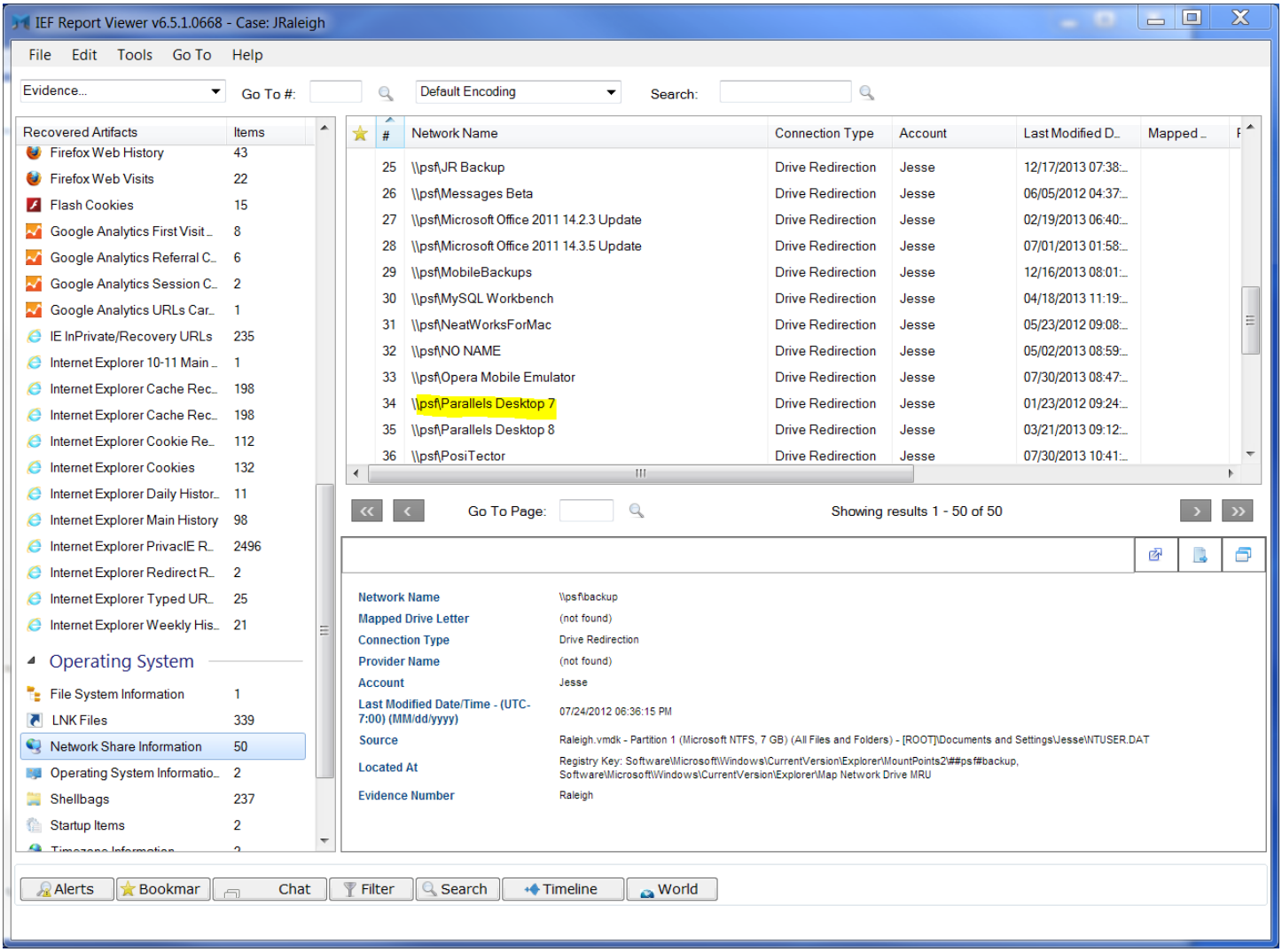
Using IEF (Internet Evidence Finder) and EnCase software I searched and identified all the videos on the drive and could not locate any responsive data. I located uTorrent client software on the machine and LNK file in the start menu of computer user Jesse.

Linked Path	C:\Documents and Settings\Jesse\Application Data\Parallels\Shared Applications\uTorrent (Mac).exe
Arguments	(not found)
Created Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/03/2011 02:58:02 PM
Last Modified Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/03/2011 02:58:02 PM
Last Accessed Date/Time - (UTC-7:00) (MM/dd/yyyy)	04/18/2013 11:19:21 AM
Target File Created Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/03/2011 02:58:02 PM
Target File Last Modified Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/03/2011 02:58:02 PM
Target File Last Accessed Date/Time - (UTC-7:00) (MM/dd/yyyy)	01/03/2011 02:58:02 PM
Target Attributes	FILE_ATTRIBUTE_ARCHIVE
Drive Type	DRIVE_FIXED
Serial Number	F4A72673
Volume Name	(not found)
Show Command	SW_SHOWNORMAL
Net Bios Name	jesse-b3e74a68a
Mac Address	00:1C:42:4E:E2:20
Target File Size (Bytes)	228864
Source	Raleigh.vmdk - Partition 1 (Microsoft NTFS, 7 GB) (All Files and Folders) - [ROOT]\Documents and Settings\Jesse\Start Menu\Programs\Parallels Shared Applications\uTorrent (Mac).lnk

Using EnCase and IEF software I searched for possible network storage locations. NetHood which corresponds to %USERPROFILE%\NetHood, contains only LAN shared folder path (server and folder name). NetHood stores the path to the folder containing shortcuts to servers that the user has added to My Network Places. This indicates additional file storage somewhere on the local network. IEF located locations on the network including "PSF" where folders are being accessed including "\\psf\Parallels Desktop" 7&8. The Parallels Desktop folder 7&8 indicate possible existence of other virtual machines or where various versions of Parallels software resides. I exported IEF's complete list of Network Share Information and Shellbags to the final report case files folder under "MacBook C02HW056DV31_JRaleigh_LT1\Windows XP Parallels Virtual Machine Files".

	Name	Physical Size	File Ext	Full Path	Is Deleted	Last Accessed	File Created
1	c on 10.10.10.42	256	42	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on 10.10.10.42	No	07/29/13 05:07:09PM	06/05/12 10:21:24PM
2	c on 10.10.10.7	256	7	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on 10.10.10.7	No	07/29/13 05:07:09PM	08/13/12 08:31:43AM
3	c on CH4 (10.10.10.39)	256	39)	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on CH4 (10.10.10.39)	No	07/29/13 05:07:09PM	06/05/12 06:40:34PM
4	c on Phillips (10.10.10.6)	256	6)	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on Phillips (10.10.10.6)	No	07/29/13 05:07:09PM	10/01/12 10:34:30AM
5	c on Swan (10.10.10.46)	256	46)	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on Swan (10.10.10.46)	No	07/29/13 05:07:09PM	06/05/12 10:25:42PM
6	Home on psf	256		RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\Home on psf	No	07/29/13 05:07:09PM	06/05/12 06:39:06PM
7	xampp on 10.10.10.8	256	8	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\xampp on 10.10.10.8	No	07/29/13 05:07:09PM	05/22/12 05:01:32PM
8	c on 10.10.10.26	256	26	RaleighVM\Raleigh\C\Documents and Settings\Jesse\NetHood\c on 10.10.10.26	No	12/16/13 10:01:23PM	05/23/12 01:45:17PM

IEF screen capture of Network Share Information for "\\psf\"



JRaleigh_RT2" aka "MacBook 340269NBATM

Time Zone Settings

JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\private\etc\localtime
Configured Time Zone:America/Detroit

```
/usr/share/zoneinfo/America/Detroit
```

OS Information

```
ProductBuildVersion: 13F34
ProductCopyright: 1983-2014 Apple Inc.
ProductName: Mac OS X
ProductUserVisibleVersion: 10.9.5
ProductVersion: 10.9.5
```

User Information

	Name	File Ext	Last Accessed	File Created	Full Path
1	.localized	localized	08/25/13 04:58:39AM	08/25/13 04:58:39AM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\.localized
2	heather		06/24/12 05:38:39PM	06/24/12 10:29:51AM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\heather
3	j		07/27/11 01:44:50PM	07/27/11 01:44:50PM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\j
4	jr		06/24/12 05:39:09PM	07/27/10 12:51:33AM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr
5	Ove		04/17/13 11:15:35PM	04/17/13 11:15:26PM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\Ove
6	Shared		02/17/14 08:26:14AM	06/13/11 12:52:36PM	JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\Shared

JRaleigh_RT2" aka "MacBook 340269NBATM Findings:

A search of the hard drive for evidence relating to Malibu Media movies was negative. A search of the hard drive evidence of BitTorrent use was positive.

1. Located several BitTorrent related website URLs pertaining to the website "The Pirate Bay". Please refer to the Final Report Case Files folder for this device "Pirate Bay URLs".

UTorrent installed on Computer

Name uTorrent
Is Deleted No
Last Accessed 12/03/14 02:16:47PM
File Created 01/30/12 09:30:08AM
Last Written 01/30/12 09:30:08AM
File Acquired 12/03/14 04:02:13PM
Physical Location388,321,886,208
Physical Sector 758,441,184
Evidence File MacBook 340269NBATM
Full Path JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Applications\uTorrent.app\Contents\MacOS\uTorrent

Numerous Music MP3 files have embedded metadata referencing "www.torrentazos.com" indicating their possible origin. The website "www.torrentazos.com" is a website where user can illegally obtain music, movies etc.

	Name	Preview	Hit Text
74	05 The Rape Over.mp3	ON East Coast RapUFID http://musicbrainz.org COMM c0 www.torrentazos.comTRCK 5/18TPOS 0APIC w image/png ‰PNG IHDR	.torrent
75	06 - I Got Bass.mp3	k On My Shit!TRCK 6TYER 2009TCON Hip-HopCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000BD1 00000B54 00003A	.torrent
76	06 - I Got Bass.mp3	k On My Shit!TRCK 6TYER 2009TCON Hip-HopCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000BD1 00000B54 00003A	.torrent
77	06 - Walk This Way.mp3	Aerosmith Devil's Got A New Disguise (Th2006www.torrentazos.com	.torrent
78	06 - Walk This Way.mp3	Walk This WayTRCK 6TYER 2006TCON RockCOMM eng www.torrentazos.comTALB 8 Devil's Got A New Disguise (The Very Best Of Aerosmith)TP	.torrent
79	06 Drive Slow (ft.Paul Wall & Glc).mp3	ate RegistrationTYER 2005TRCK 6TCON (15)COMM spa www.torrentazos.comTPE1 Kanye WestCOMM h engiTunNORM 0000080E 0000085B 000	.torrent
80	06 Hate that I Love You (Feat. Ne-Yo).mp3	ood Girl Gone BadTRCK 6TYER 2007TCON R&BCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000A85 00000BC2 00003	.torrent
81	06 Metal Heart.mp3	Bleed Like MeTRCK 6TYER 2005TCON RockCOMM $ eng www.torrentazos.com By FEFE2003APIC dD image/png ‰PNG IHDR ô ä ß% È	.torrent
82	06 Nothing's The Same.mp3	006TCON Hard RockUFID http://musicbrainz.org COMM c0 www.torrentazos.comTXXX MusicBrainz Artist Id TXXX musicbrainz_artistid TRC	.torrent
83	06 Silver.mp3	Rain TRCK 6 TYER 2007 TCON Heavy Metal COMM eng www.torrentazos.com	.torrent
84	07 - Dude (Looks Like A Lady).mp3	dy) Aerosmith Devil's Got A New Disguise (Th2006www.torrentazos.com	.torrent
85	07 - Dude (Looks Like A Lady).mp3	oks Like A Lady)TRCK 7TYER 2006TCON RockCOMM eng www.torrentazos.comTALB 8 Devil's Got A New Disguise (The Very Best Of Aerosmith)TP	.torrent
86	07 - Girls Love Me feat. Rick Ross.mp3	k On My Shit!TRCK 7TYER 2009TCON Hip-HopCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000FCF 00001150 00007F	.torrent
87	07 Bedstuy Parade & Funeral March.mp3	ON East Coast RapUFID http://musicbrainz.org COMM c0 www.torrentazos.comTRCK 7/18TPOS 0APIC w image/png ‰PNG IHDR	.torrent
88	07 Civilize The Universe.mp3	Rain TRCK 7 TYER 2007 TCON Heavy Metal COMM eng www.torrentazos.com	.torrent
89	07 Hell Is High.mp3	hot To HellTRCK 7TYER 2006TCON Hard RockCOMM eng www.torrentazos.comTLAN engCOMM h engiTunNORM 00002359 00002EDE 0000910D	.torrent
90	07 My Way Home (ft.Common).mp3	ate RegistrationTYER 2005TRCK 7TCON (15)COMM spa www.torrentazos.comTPE1 Kanye WestCOMM h engiTunNORM 000004D8 000004D9 000	.torrent
91	07 Say it.mp3	ood Girl Gone BadTRCK 7TYER 2007TCON R&BCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000972 00000942 00006	.torrent
92	07 Sex Is Not The Enemy.mp3	Bleed Like MeTRCK 7TYER 2005TCON RockCOMM $ eng www.torrentazos.com By FEFE2003APIC dD image/png ‰PNG IHDR ô ä ß% È	.torrent
93	07 What Else Is There.mp3	05TCON ElectronicUFID http://musicbrainz.org COMM " c0 www.torrentazos.com By FEFETRCK 7TPOS 0TLAN EnglishCOMM h engiTun	.torrent
94	08 - Blown feat. T-Pain.mp3	k On My Shit!TRCK 8TYER 2009TCON Hip-HopCOMM eng www.torrentazos.comTLAN EnglishCOMM h engiTunNORM 00000804 00000830 00004A	.torrent
95	08 - Rag Doll.mp3	Aerosmith Devil's Got A New Disguise (Th2006www.torrentazos.com	.torrent
96	08 - Rag Doll.mp3	2 Rag DollTRCK 8TYER 2006TCON RockCOMM eng www.torrentazos.comTALB 8 Devil's Got A New Disguise (The Very Best Of Aerosmith)TP	.torrent

Located Torrent Files

1) File Name: cablegate-201011290900.7z.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 11/29/10 08:18:17AM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\cablegate-201011290900.7z.torrent

2) File Name: Chinga La Migra.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 06/24/11 09:39:07AM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\Chinga La Migra.torrent

3) File Name: Chinga_La_Migra_Dos.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 06/29/11 10:27:31AM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\Chinga_La_Migra_Dos.torrent

4) File Name: MMM_Booz_Allen.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 07/11/11 02:34:41PM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\MMM_Booz_Allen.torrent

5) File Name: NeoOffice-3.1.2-Intel.dmg.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 02/11/11 11:37:50PM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\NeoOffice-3.1.2-Intel.dmg.torrent

6) File Name: Zenith.Part.1.2011.720p.x264-VODO.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 03/20/11 09:09:03AM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\Zenith.Part.1.2011.720p.x264-VODO.torrent

7) File Name: sDgo3FDksdGwsrkrS.enc.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 08/31/11 02:30:15PM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\sDgo3FDksdGwsrkrS.enc.torrent

8) File Name: cablegate-201108300212.7z.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 09/02/11 12:07:41AM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\cablegate-201108300212.7z.torrent

9) File Name: 404EC54D29D940D04485756D7500745F8CFF10C3.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 02/07/12 12:02:12AM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\404EC54D29D940D04485756D7500745F8CFF10C3.torrent

10) File Name: American Survival Guide Magazine.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 03/03/12 12:17:16PM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\American Survival Guide Magazine.torrent

11) File Name: BT5R2-GNOME-32.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 05/05/12 11:07:56PM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\BT5R2-GNOME-32.torrent

12) File Name: THE METEORS - [WWW.PunksAndSkins.COM] - 13 ALBUMS.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 06/06/12 11:02:29PM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\THE METEORS - [WWW.PunksAndSkins.COM] - 13 ALBUMS.torrent

13) File Name: Demented Are Go.torrent
Last Accessed: 06/22/12 02:02:02PM
File Created: 06/06/12 11:19:35PM
Full Path: JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Users\jr\Library\Application Support\uTorrent\Demented Are Go.torrent

Located USB Device Connection Information

Using EnCase software I conducted a keyword search of the "system.log" files located on both laptop computers using the keyword "USBMSC". Using the keyword "USBMSC" I was able to locate and identify USB devices that were plugged into the laptop computers. The following is a bookmark list of the keyword search hits.

1) File Name: system.log.0 (Zip File Volume)
Last Accessed: 12/03/14 01:25:13AM
File Created: 12/03/14 01:25:13AM
Comments: Identified as a Western Digital Technologies, Inc. My Book Essential (WDBACW) (External USB Hard Drive 1-3TB in size depending on the exact model) Keyword searching indicates a model "1140" which is a 2TB hard drive.
Full Path: JRaleigh\MacBook C02HW056DV31\D\Macintosh HD\private\var\log\system.log.0.gz\GZIP Volume\system.log.0

```
Dec  2 08:27:16 jrmbp kernel[0]: USBMSC Identifier (non-unique): 574D415A4139303734343136 0x1058 0x1140 0x1012,
```

In order to decode the values associated with these entries you need to look at the source code for IOUSBInterface.cpp from opensource.apple.com. Using the above note data you can see that the three values: 0x1058 0x1140 0x1012 are the Vendor ID, Product ID and the Device Release number:

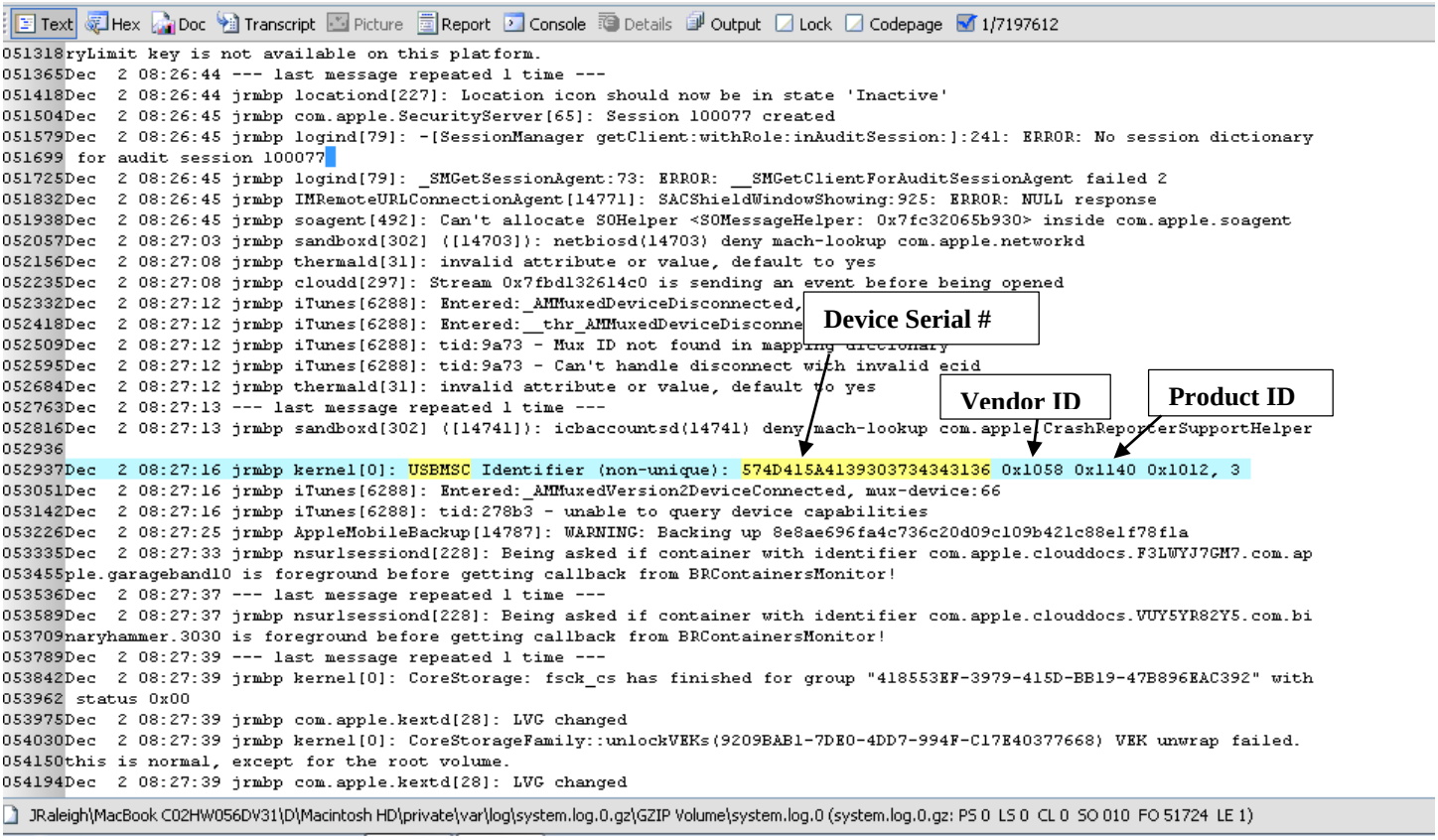
```
// these properties come from the device descriptor, but can be used for interface matching
    setProperty(kUSBVendorID, (unsigned long long)_device->GetVendorID(), (sizeof(UInt16) * 8));
    setProperty(kUSBProductID, (unsigned long long)_device->GetProductID(), (sizeof(UInt16) * 8));
    setProperty(kUSBDeviceReleaseNumber, (unsigned long long)_device->GetDeviceRelease(), (sizeof(UInt16) * 8));
```

In this case looking online at the most up to date database: http://www.linux-usb.org/usb.ids one can see that 0x1058 (1058) is from Western Digital Technologies, Inc. and 0x1140 (1140) is a My Book Essential (WDBACW) and 0x1012 (1012) is the release for that drive.

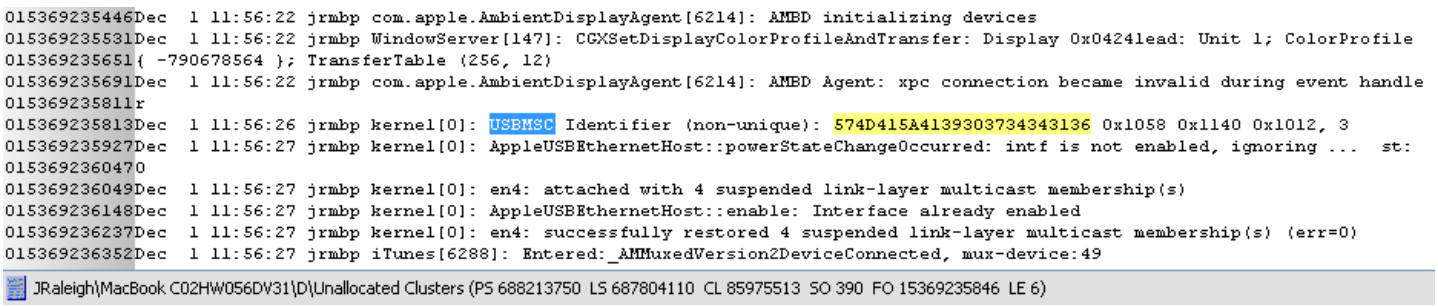
Using EnCase software I conducted a keyword search for serial number "574D415A4139303734343136" pertaining to the Western Digital My Book Essentials External USB hard drive. I located evidence that this device was plugged into both laptop computers numerous times. The search hits were exported out and are viewable by reviewing the final report case files folder named "USB Device Search Hits".

1. **JRaleigh_LT1" aka "MacBook C02HW056DV31** – Numerous search hits in the Parallels.log file, unallocated space and "2014.12.02.U0.G80.asl" indicate evidence of connection from 7/10/2013 to 12/2/2014.
2. **JRaleigh_RT2" aka "MacBook 340269NBATM** – Numerous search hits in the Parallels.log file, unallocated space and "dispatcher.desktop.xml" indicate evidence of connection from 10/13/2011 to 2/17/2014.

EnCase Screen Captures of the system.log file JRaleigh_LT1" aka "MacBook C02HW056DV31 from 12/2/2014



EnCase Screen Captures of the system.log file JRaleigh_LT1" aka "MacBook C02HW056DV31 from 12/1/2014



EnCase Screen Captures of a Parallels.log file in unallocated space JRaleigh_LT1" aka "MacBook C02HW056DV31 from 12/16/2013

```
00815013568712-16 12:57:52.505 F /gui:343:707/ localhost: received result for [DspCmdUserGetHostHwInfo]. RC = [PRL_ERR_SUCCESS]
00815013580312-16 12:57:57.315 F /disp:656:8303/ On enter : dev_type = 15  dev_name = 15100000  event_code = 1
00815013590212-16 12:57:57.541 F /disp:656:8303/ USB connected (autoconnect) <15100000|1058|1140|super|--|574D415A4139303734343136>
00815013602<My Book 1140> <PUDT_DISK_STORAGE>
00815013605712-16 12:57:57.542 F /disp:656:8303/ USB GUI notify '' <15100000|1058|1140|super|--|574D415A4139303734343136> <My Book 1
00815013617140> <PUDT_DISK_STORAGE>
00815013620212-16 12:57:57.544 F /disp:656:8303/ make post to autoconnect event from thread notifier! strDevImage == 15100000|1058|1
00815013632140|super|--|574D415A4139303734343136 uiDevState==1
00815013637412-16 12:57:57.546 F /disp:656:8303/ USB VM notify 'connect' <15100000|1058|1140|super|--|574D415A4139303734343136> <My
00815013649Book 1140> <PUDT_DISK_STORAGE>
00815013652512-16 12:57:57.547 F /disp:656:8303/ make post to autoconnect event from thread notifier! strDevImage == 15100000|1058|1
00815013664140|super|--|574D415A4139303734343136 uiDevState==1
00815013669712-16 12:57:57.550 F /disp:656:8303/ usb device with id == 15100000|1058|1140|super|--|574D415A4139303734343136 removed
00815013681from list excluded of autoconnect
00815013685112-16 12:57:57.551 F /gui:343:707/ localhost: received event PET_DSP_EVT_HW_CONFIG_CHANGED, code = [100202]
00815013695912-16 12:57:57.555 F /gui:343:707/ localhost: sending [DspCmdUserGetHostHwInfo] request...
00815013705012-16 12:57:57.555 D /disp:656:a01f/ Processing command 'DspCmdUserGetHostHwInfo' 2051 (PJOC_SRV_GET_SRV_CONFIG)
```

JRaleigh\MacBook C02HW056DV31\D\Unallocated Clusters (PS 193845315 LS 193435675 CL 24179459 SO 144 FO 8150136464 LE 24)

EnCase Screen Captures of a Parallels.log file in unallocated space from JRaleigh_RT2" aka "MacBook 340269NBATM Dated 11/24/2012

```
22650078d Reader> <PUDT_DISK_STORAGE>
22650108 11-24 15:48:34.146 I /pvsHostInfo:245:690b/ LOOKUP1 <26400000|1058|1140|high|--|574D415A4139303734343136> <My Book 1140>
22650228  <PUDT_DISK_STORAGE>
22650249 11-24 15:48:34.182 F /disp:245:690b/ USB connected <26400000|1058|1140|high|--|574D415A4139303734343136> <My Book 1140>
22650369<PUDT_DISK_STORAGE>
22650389 11-24 15:48:34.220 F /disp:245:690b/ make post to autoconnect event from thread notifier! strDevImage == 26400000|1058|1
22650509140|high|--|574D415A4139303734343136 uiDevState==1
22650560 11-24 15:48:34.236 F /disp:245:690b/ make post to autoconnect event from thread notifier! strDevImage == 26400000|1058|1
22650680140|high|--|574D415A4139303734343136 uiDevState==1
22650731 11-24 15:48:34.244 F /disp:245:690b/ usb device with id == 26400000|1058|1140|high|--|574D415A4139303734343136 removed f
22650851rom list excluded of autoconnect
22650884 11-24 15:48:34.471 F /disp:245:690b/ On exit  : dev_type = 15  dev_name = 26400000  event_code = 1
22650983 11-24 15:48:38.467 F /disp:245:690b/ On enter : dev_type = 6  dev_name = IOMedia  event_code = 0
22651080 11-24 15:48:38.467 F /disp:245:690b/ Device change: host hardware info refreshing was skipped !
22651176 11-24 15:48:38.482 F /disp:245:690b/ On exit  : dev_type = 6  dev_name = IOMedia  event_code = 0
22651273 11-24 15:48:38.482 F /disp:245:690b/ On enter : dev_type = 15  dev_name =   event_code = 0
22651364 11-24 15:48:38.485 I /pvsHostInfo:245:690b/ LOOKUP1 <24600000|05ac|8507|high|--|8JA6N2E5JDCLNA00> <Apple Built-in iSight
22651484> <PUDT_VIDEO>
22651499 11-24 15:48:38.488 I /pvsHostInfo:245:690b/ LOOKUP1 <6300000|05ac|0236|full|KM|Empty> <Apple Internal Keyboard / Trackpa
22651619d> <PUDT_KEYBOARD>
22651638 11-24 15:48:38.489 I /pvsHostInfo:245:690b/ LOOKUP1 <6500000|05ac|8242|low|--|Empty> <Apple IR Receiver> <PUDT_COMMUNICA
22651758TION>
22651764 11-24 15:48:38.489 I /pvsHostInfo:245:690b/ LOOKUP1 <6610000|05ac|8213|full|--|5C5948C71E36> <Apple Bluetooth USB Host C
22651884ontroller> <PUDT_BLUETOOTH>
22651912 11-24 15:48:38.492 I /pvsHostInfo:245:690b/ LOOKUP1 <26100000|05ac|8403|high|--|000000009833> <Apple Internal Memory Car
22652032d Reader> <PUDT_DISK_STORAGE>
22652062 11-24 15:48:38.505 F /disp:245:690b/ USB disconnected <26400000|1058|1140|high|--|574D415A4139303734343136> <My Book 114
226521820> <PUDT_DISK_STORAGE>
22652205 11-24 15:48:38.507 F /disp:245:690b/ make post to autoconnect event from thread notifier! strDevImage == 26400000|1058|1
22652325140|high|--|574D415A4139303734343136 uiDevState==0
22652376 11-24 15:48:38.919 F /disp:245:690b/ On exit  : dev_type = 15  dev_name =   event_code = 0
22652467 11-24 15:53:31.527 I /prl_time_machine_helper:245:307/ The Time Machine start up notification was recieved
22652574 11-24 16:39:41.273 F /disp:245:6a03/ System events monitor: host going to sleep, prepare
22652663 11-24 16:39:41.273 F /disp:245:6a03/ System events monitor: host going to sleep, done
```

JRaleigh\MacBook 340269NBATM\1 Macintosh HD\Macintosh HD\Library\Logs\parallels.log (PS 658973880 LS 658564240 CL 82320530 SO 358 FO 22651238 LE 1)

Toshiba External Hard Drive with NTFS Windows Partition

Looking at the screen capture below and referring to the most up to date database: http://www.linux-usb.org/usb.ids one can see that 0x048 (0480) is from Toshiba America Info. Systems, Inc. and 0x200 (0200) is an External Disk and 0x0 (00) is the release for that device. I located 1 entry for this device.

EnCase Screen Captures of a System.log file in unallocated space JRaleigh_LT1" aka "MacBook C02HW056DV31 from 10/15/2014

```
057007532882Oct 15 14:45:51 jrmbp Slack[576]: CGSCopyDisplayUUID: Invalid display 0x0424lead
057007532963Oct 15 14:45:51 jrmbp Slack[576]: CGSCopyDisplayUUID: Invalid display 0x78c59245
057007533044Oct 15 14:45:54 jrmbp kernel[0]: USBMSC Identifier (non-unique): 20140618002698F 0x480 0x200 0x0, 3
057007533144Oct 15 14:45:56 jrmbp Flu[431]: Display list confused, doing full reset.
057007533218Oct 15 14:45:59 jrmbp com.apple.kextd[19]: Can't create kext: invalid CFBundleVersion in identifier cache entry entry 34
057007533338 9.
057007533341Oct 15 14:45:59 --- last message repeated 1 time ---
057007533394Oct 15 14:45:59 jrmbp com.apple.kextd[19]: kext com.github.osxfuse.filesystems.osxfusefs  204029000 is in exception list
057007533514, allowing to load
057007533533Oct 15 14:45:59 jrmbp kernel[0]: OSXFUSE: starting (version 2.4.2, Jun  6 2012, 13:39:25)
057007533623Oct 15 14:45:59 jrmbp ntfs-3g[5940]: Version 2010.10.2-mac external FUSE 27
057007533699Oct 15 14:45:59 jrmbp ntfs-3g[5940]: Mounted /dev/rdisklsl (Read-Write, label "TOSHIBA EXT", NTFS 3.1)
057007533802Oct 15 14:45:59 jrmbp ntfs-3g[5940]: Cmdline options: norecover,nfconv,auto_xattr,local,defer_permissions
057007533908Oct 15 14:45:59 jrmbp ntfs-3g[5940]: Mount options: auto_xattr,local,defer_permissions,allow_other,nonempty,relatime,fsn
057007534028ame=/dev/disklsl,volname=TOSHIBA EXT
057007534065Oct 15 14:45:59 jrmbp ntfs-3g[5940]: Ownership and permissions disabled, configuration type 1
057007534159Oct 15 14:46:00 jrmbp fseventsd[54]: could not open <</Volumes/TOSHIBA EXT/.fseventsd/fseventsd-uuid>> (No such file or
057007534279directory)
057007534290Oct 15 14:46:00 jrmbp fseventsd[54]: log dir: /Volumes/TOSHIBA EXT/.fseventsd getting new uuid: A1FED691-0C9E-450F-9E31-
057007534410 4612FE188309
057007534423Oct 15 14:46:00 jrmbp com.apple.kextd[19]: Can't create kext: invalid CFBundleVersion in identifier cache entry entry 34
057007534543 9.
057007534546Oct 15 14:46:15 --- last message repeated 5 times ---
057007534600Oct 15 14:46:15 jrmbp diskarbitrationd[60]: unable to mount /dev/disklsl (status code 0xFFFFFFFE).
057007534699Oct 15 14:46:15 jrmbp mds[44]: (Normal) Volume: volume:0x7fac28ad7000 ********** Bootstrapped Creating a default store:1
057007534819  SpotLoc:(null) SpotVerLoc:(null) occlude:0 /Volumes/TOSHIBA EXT
057007534884Oct 15 14:46:51 jrmbp Slack[576]: CGSCopyDisplayUUID: Invalid display 0x5b81c5c1
057007534965Oct 15 14:46:51 jrmbp Slack[576]: CGSCopyDisplayUUID: Invalid display 0x0424lead
```

JRaleigh\MacBook C02HW056DV31\D\Unallocated Clusters (PS 1420225374 LS 1419815734 CL 177476966 SO 113 FO 57007533169 LE 1)

IPad Devices & Findings

On the hard drive I was provided were Cellebrite extractions for 2 Apple iPad devices. Both devices were searched using Cellebrite's Physical Analyzer software. The search was negative for Malibu Media's works and for BitTorrent use and related activity.

1. iPad1_5.1-5.1.1_Physical_05-12-14_10-03-39
2. AppleDevice_AdvancedLogical_09-12-14_11-52-17